

1L04/904



מדינת ישראל  
STATE OF ISRAEL

REC'D 01 NOV 2004

WIPO

PCT

Ministry of Justice  
Patent Office

משרד המשפטים  
לשכת הפטנטים

This is to certify that  
annexed hereto is a true  
copy of the documents as  
originally deposited with  
the patent application  
particulars of which are  
specified on the first page  
of the annex.

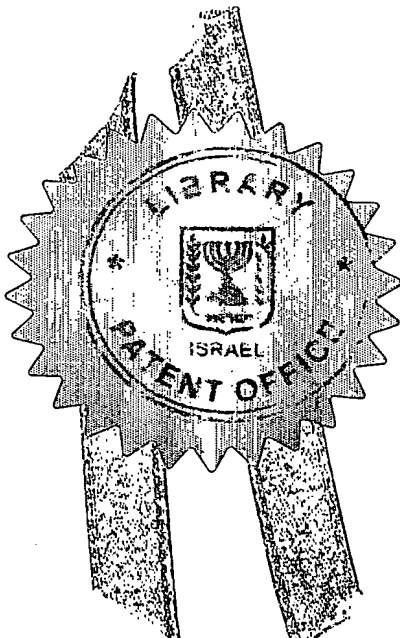
זאת לתעודה כי  
רצופים בזה העתקים  
נכונים של המסמכים  
שהופקדו לכתחילה  
עם הבקשה לפטנט  
לפי הפרטים הרשומים  
בעמוד הראשון של  
הנספח.

**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

14-10-2004

This document is  
מ. לטדי  
ממנה על הבורחים  
הפטנטים

Commissioner of Patents



נתאשר  
Certified

לשימוש הלשכה  
For Office Use

מספר: Number	158207
תאריך: Date	01-10-2003
הוקדם/נדחה: Ante/Post-dated	

**בקשה לפטנט**  
Application For Patent

אני, (שם המבקש, מענו ולגבי גוף מאוגד - מקום התאגדותו)  
I, (Name and address of applicant, and in case of body corporate-place of incorporation)

W.E.C.U. Technologies Ltd. באמצעות שרון ארליך, ת.ד. 599, כפר ויתקין 40290, ישראל.  
W.E.C.U. Technologies Ltd. By Sharon Erlich, of P.O.Box 599, Kfar Vitkin 40290, ISRAEL

The Inventors: Sharon ERLICH Boaz GANOR בועז גנור שרון ארליך הממציאים:  
Eli BARNEA Zipora ALSTER ציפורה אלסטר אלי ברנע  
Shlomo BREZNITZ Ehud GIVON אהוד גבעון שלמה ברזניץ

ששמה הוא Right of Law הדין בעל אמצאה מכח  
of an invention the title of which is Owner, by virtue of

מערכת ושיטה לאיתור וסינון אנשים שיש להם מה להסתיר

(בעברית)  
(Hebrew)

Method and System for Locating and Screening individuals with Hidden intent

(באנגלית)  
(English)

Hereby apply for a patent to be granted to me in respect thereof.

מבקש בזאת כי ינתן לי עליה פטנט

* בקשת חלוקה Application of Division		* בקשת פטנט מוסף Appl. for Patent of Addition		דרישת דין קדימה Priority Claim	
מבקשת פטנט from application		* לבקשה/לפטנט to Patent/Appl.		מספר/סימן Number/Mark	מדינת האיגוד Convention Country
No. _____	מס' _____	No. _____	מס' _____	תאריך Date	
Dated _____	מיום _____	Dated _____	מיום _____		
P.O.A.: _____		* יפוי כח: _____			
C. 148435		המען למסירת מסמכים בישראל Address for Service in Israel			
REINHOLD COHN AND PARTNERS Patent Attorneys P.O.B. 4060, Tel-Aviv		ריינהולד כהן ושותפיו עורכי פטנטים ת"ד 4060, תל-אביב			
חתימת המבקש Signature of Applicant		בשם המבקשים, ריינהולד כהן ושותפיו ע"י: -		שנת 2003 Year	בחודש October of
				היום 1 This	
				לשימוש הלשכה For Office Use	

טופס זה כשהוא מוטבע בחותם לשכת הפטנטים ומושלם במספר ובתאריך ההגשה, הוא אישור להגשת הבקשה שפירוט רשומים לעיל.  
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application the particulars of which are set out above.

\* מחק את המיותר  
Delete whatever is inapplicable

מערכת ושיטה לאיתור וסינון אנשים שיש להם מה להסתיר

## Method and System for Locating and Screening individuals with Hidden intent

W.E.C.U. Technologies Ltd.

W.E.C.U. Technologies Ltd.

### The Inventors:

Sharon ERLICH

Eli BARNEA

Shlomo BREZNITZ

Boaz GANOR

Zipora ALSTER

Ehud GIVON

### הממציאים:

שרון ארליך

אלי ברנע

שלמה ברזניץ

בועז גנור

ציפורה אלסטר

אהוד גבעון

C. 148435

# **METHOD AND SYSTEM FOR LOCATING AND SCREENING INDIVIDUALS WITH HIDDEN INTENT**

5

## **FIELD OF THE INVENTION**

10 This invention, in general, deals with locating and screening individuals with hidden intent, before acting, during the preparations, while carrying out the act, and after.

## **BACKGROUND OF THE INVENTION**

15 The need to locate individuals with hidden malicious intent is the basis for the use of access control systems.

In many cases, the verification of the individual identity, luggage x-ray examination, and random physical search are not sufficient, as in access control of sea and air ports (for example). In such cases, there is a conflict between the need to transport large masses of people (which requires fast response) and the ability to distinguish  
20 individuals with hidden malicious intent, and detain them (which slows down the process in cases of extensive search).

Many systems were developed to provide a solution, such as:

- 25 a. Chemical sniffers – This method uses sensors that identify the remains of suspicious materials. This method is limited to the identification of pre-known materials that the system can identify, and that are not camouflaged.
- b. Metal sensors – This method uses sensors that identify metal objects that are  
30 hidden on the tested subject's body or inside his luggage. This method is limited to the identification of metallic materials only.
- c. Electromagnetic and X-ray radiation sensors - This method uses the absorption / transference characteristics of materials to different types of radiation, in

order to create an image that reflects the subject or his luggage. This method is elaborating from day to day, and provides reliable information. Still, it does not cover subjects with malicious intent that do not carry deadly weapons, or do carry hazardous materials and camouflaged objects that the human inspector can not decipher by looking at the screen.

- d. Biometric sensors - This method uses sensors that identify the tested subject's personal characteristics (fingerprints, reticulum image, etc.) in order to decisively verify his identity even in case of impersonation. This is a developing technology, but its main disadvantage is of its inability to locate individuals with malicious intent that are not marked in advance by the system (by intelligence information or otherwise). Some of the biometrics sensors also can not distinguish abiosis in the tested parameter.
- e. Physiological sensors - This method uses sensors that identify different physiological parameters which indicate stress (heart pace, GSR, blood pressure, voice spectrum, etc.) These systems partially require a physical contact of the individual with the system. Also, they are nor fully reliable and open to circumvention by a trained person.
- f. Animals (bees, fish and others) behavioristic sensors - This method uses the ability of some animals to identify stress. These methods are slow and unreliable.
- g. Behaviorist sensors - This method uses sensors that identify behaviorist parameters (stammering, associations, etc.). Theses methods are unfounded within large populations, and are limited as a single indicator for prediction.

All the reviewed systems are characterized with one or more of the following, which limits their effectiveness:

- Limited current know-how
- Dependence upon intelligence or other early information
- Unreliable results

- Slow operation

There is a need in the art to provide for a system and method for locating people with hidden intent, without significant disturbance to mass traffic and with minimum false alarms.

## BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding, the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 illustrates a flow chart of generalized sequence of test selection operation, in accordance with an embodiment of the invention;

Fig. 2 illustrates a flow chart of generalized sequence of test example operation, in accordance with an embodiment of the invention; and

Fig. 3 illustrates a generalized block diagram of exemplary system architecture, in accordance with an embodiment of the invention.

## DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

In accordance with certain embodiment, the system is composed of a few major elements:

- I. Identity verification system/s (by documents, pictures, and/or different types of biometric sensors)
- II. Transparency and sensing tools (one or more), to check the tested subjects' body and luggage: metal sensors, chemical sniffers to detect: explosives, HAZMATS, drugs, etc., biological sensors to detect bacteria, and more.
- III. Physiological test systems: reaction to simulations, stress, reaction to drugs, and more. Such systems might require direct contact of the tested subject with the sensors, or be operated from distance without touch.

IV. Routing devices, as well as suspect neutralization systems (detaining, shock) that are explosion proof and protect the crowd and the security personnel.

5 The system has one or more measuring points, where the tested subject goes through at least two similar tests, behaviorist and/or physiological. The difference between the two measurements is a manipulation, open or concealed, that appears before or during one of the measures. The results of the measures are analyzed in at least one of three levels: First, against general population data, second - within  
10 subject, that allows to detect the changes resulting the manipulation, and third, analyzing against prior data gathered about the tested subject by similar systems in the past. The nature of the manipulation is planned to target the subject who understands the significance of the manipulation and can react to it. (For example, stressing manipulations: a picture of drugs syringe and a policeman - targeting a drugs dealer, a  
15 picture of an Islamic leader or symbol - targeting Islamic terrorists. Facing, a calming manipulation: a picture of a peaceful escape resort in the islands - targeting a suspect on the run).

The focused manipulation matches the required identification, and creates physiological and/or behaviorist changes among the targeted subjects and by that  
20 separates them from the general public.

The manipulations, as well as the tested parameters, are chosen automatically (possibly using random or pseudo-random selection of manipulation from manipulation bank) or manually by the system, and by one embodiment the human operator may not have influence, or knowledge about the manipulation and of the  
25 measured parameters. The only part of the system that the field operator is aware of is the alarm/clearance signal as to the tested subject. Note that the lack of knowledge of the exact manipulation that will be invoked hinders on the likelihood of deceiving or "cheating" the system. Thus, on absent of knowing the precise manipulation that the individual is subjected to, he (or she) is unable to conduct a preparatory training in  
30 which the individual is trained to control the psychological/ behaviorist parameters when being subjected to a given manipulation.

The system has a manipulation bank, which includes a wide variety of manipulations that might be:

- Open or concealed
- Stressing or relaxing
- Creating conscience or sub conscience reaction
- Targeted or general

5 The appearance of the different manipulations can be random (pseudo random) or scheduled, according to the algorithm activated by the system computer.

Examples for possible manipulations:

10 1) Focused, sub conscience, concealed, stressing manipulation: Flashing a symbol known only to the target, inside a screen which is observed by the tested subject, and is subconsciously perceived by his mind.

15 2) General, conscience, open, stressing manipulation:  
Security inspector posted at the check point.

20 By this embodiment, the system is operated by software that receives data from its internal sources, and may as well receive data from outside sources (government data bases, luggage screening systems, etc.). The system examines the data in relation to itself (including historical data of the tested subject) and in relation to the general population.

25 The tested parameters, beyond the statistical measurements (such as transparency, biometrics, sniffing, etc.) are by this embodiment physiological without touch (photographing pupil size, voice analyzing) and/or behaviorist (for example, associative sequence).

The system's decisions are based, as much as possible, upon more than one parameter, in order to increase its reliability.

30 The system is an adaptive system that uses its accumulative data to update parameters for on-going sectioning and analyzing, improving its decisions (decreasing false alarms of both types – false positive and false negative), shortening decision time, diluting parameters, etc.

Note that the invention is not bound by these specific system characteristics.



Examples for possible usage of the system:

A. Airport, locating drugs smugglers

5           A.1. General:

A passenger or accompanier, who becomes a tested subject, enters the airport and goes through routed channels, in order to minimize the damage in case of violence, self explosion or any other aggressive activity that might threaten his surroundings.

10       The instructions while going through the site might be given by an automatic system and/or human inspectors. Such presence of security personnel might be part of the manipulations in addition to their traditional roll in the general security of the site. (Note: according to American regulations, at least one of the tests should not demand seeing by the subject, or be replaced by an auditorial alternative.)

15

A. 2. An example of test procedure:

1. The tested subject enters the airport through the entrance gate.
2. At the first check point, the subject is tested by sensors that check what he is  
20       carrying on his body, as well as his luggage (Looking for metals, firearms and cold weapons, explosives, HAZMATS, etc.). The sensors that are activated are chosen by the system computer, by software that receives data from the active systems (Plug and Play), and accesses to the Data Base for retrieving the parameters of the active systems. The subject, as well as the operators of the  
25       system, does not know whether, or which system is going to be activated, and whether or which kind of manipulation will appear. Thus, the subject is not able to plan his reaction in order "to please" the system and modify the results.
3. Following (and/or simultaneously, and/or before) the above sensing procedure, the tested subject goes through documents inspection, as well as biometric  
30       tests (for example: pupil photography system - IrisAccess™ 3000 by LG; fingerprints and access control systems - DaonEngine and DaonAccess) that are also chosen without human interference by the system computer, in order to decisively verify the identity of the subject.

4. The subject is asked to answer, by pressing a key board or using a biometric mouse (BioControl BioMouse, Emotion Mouse, Unmatch Mouse), several questions that are presented over the computer screen. Some of the questions are informative, and others are associative. Simultaneously, through the screen, his pupils and face are photographed and analyzed as to changes resulting stress or excitement: Pupil size, facial expressions and temperature. In addition, his identity data, such as fingerprints and retina image, as well as physiological and behaviorist data such as GSR (rise in conductivity resulting stress), temp, heart pace, etc. are transferred together with other related data into the system computer. The computer analyzes, verifies and compares the data with existing personal information referring to the subject (prior tests, personal information, intelligence information, etc.).
5. Simultaneously, the tested subject is asked by the system several simple questions, which he has to answer in loud. His voice is recorded and analyzed in order to create a voice base line, which includes speech spectrum and voice rattling (Sub-Tremor) that are analyzed and stored in the system computer (Examples: Systems that match the criteria describes in DoDPI Research division Report, #DoDPI01-R-0001; Real-time, multi sources analyzing system, such as TiPi6 or GK1 by Namesysco Ltd.)
6. In case the subject passes the documents and identity verification as well as the transparent (X-Ray systems) and sensing procedures (For example, based on Raman Spectroscopy analysis), and also receives intelligence clearance (the system doesn't have any intelligence alarm regarding him), he can go on in the standard lane.
7. Later on the lane there is another check point that receives data from the system computer. The subject goes through additional identity verification, and again is asked to answer a computerized questionnaire, by pressing a key board. This questionnaire is opened with a notification (for example) saying: "Currently there is an operation going on in this airport, for the identification of drugs smugglers. Two smugglers have been already identified..." at the same time, the system flashes a short frame, as a concealed, sub concisions manipulation, showing a picture of the drugs baron which is suspected to be connected with the target. The manipulation is selected by the system out of

the manipulation bank, according to the data accumulated. The system might also present to the subject a voice question, in order to get a verbal response.

8. The system examines and analyzes the parameters received from the biometric mouse, in case it has chosen to use it. It also photographs the face and pupils of the subject, and analyzes his voice again. The changes in the physiological parameters, (for example: a rise or decline in heart pace, changes in GSR - potency and length of the reaction, changes in pupil size, facial expressions and temp), together with voice spectrum and Sub-Tremor are the base to the evaluation. The system evaluates whether there is a significant difference between the first and the second measurements, what is the status of the subject against typical population, and in case the data exists, what are the differences between the current and prior tests of the subject. The statistical analysis is based on Within Subject Changes analyzing tools, which enable revisal of minor changes of the subject in minimum test repetitions. That is when the data is gathered from general sources, as well as from specific detections conducted the same day in the airport, in case of significant environmental conditions.

9. The system alerts for a suspect in case the subject was graded with a mark that was defined as suspicious (for example  $\Rightarrow 0.8$ ) by one or more of the test tools, while the grade for evaluation is calculated according to the formula:

$Z = \text{sum of } (K1 \text{ to } Kn) / n$ , when:

Z – Evaluation grade

K – Ascription grade in specific test

N – Number of tests

In case of a lower grade in one or more of the tests, the criterion for decision is a sum of more than 0.7 (also for example). In case of lack of response in one of the tests (for example, a deaf person in a hearing test), the system decides according to M parameters out of N tests that were activated. This kind of decision also can be received out of the decision process of the computer system (as part of the random process, in which the subject, above all, doesn't know which tests are taken into consideration and calculated for the final grade). This sample is only one of the possible ways to establish the processing system.

10. In case the system finds suspicious reactions of the subject to the manipulations, or there isn't a complete match between the documents and the biometric data, or there is a significant difference between the current and prior tests, the system gives an alarm signal. The subject is directed to a separate and protected area, where he goes through an extensive check-up and neutralized in case of a threat such as self-explosion or shootings.

Those versed in the art will readily appreciate that the invention is not bound by this specific sequence of operations of this non limiting example.

#### A. 3. General remarks and expansions:

i. In case the authorities of an air-port are getting prepared to meet terrorist threats, for example, the manipulations will match terrorists' parameters.

ii. Combined manipulations can also be provided. They can be open and concealed, and might include more than one discipline (as an effective manipulation for smugglers and a concealed and effective manipulation for terrorists).

Combined manipulations enable to create also differential situations that isolate phenomenon, such as: a person who is infected with bacteria and isn't aware of it, but does know that he is about to meet with people who belong to a terrorist organization.

iii. The manipulation selection process can be done according to the personal data of the tested subject, such as: identity, history, origin, religion, profession, etc. In addition, the system is updated with the subject traveling information, as flights, transfer, destination, traveling history and more.

iv. Identity biometric verification might be based upon one or more biometric tools, as fingerprints, retina image (for example, Dartagnan™ biometric system), radiation and electrical fields that uniquely characterize a subject. Additionally, the test might include results verification means, such as vitality detection in the tested parameters. (For example: combining retina image test with electrical field test, which enables to determine whether the tissue observed is abiosis.)

v. A subject might be tested also while leaving the protected site, regarding his activities during his stay at the site. The system can ask him about accepting or

leaving a package, meeting with another person, etc. this is done similarly to the procedure described above.

vi. The testing procedure might be performed in one or more testing points.

5 vii. The operators of the system, as well as the security personnel, might be aware of the nature and the structure of the system, but might also not be, in order to create a situation of Double Blind Test. This means that the tested subject or his operators can not protect themselves from the system by learning about it beforehand, using intelligence observations, inside cooperation, etc.

10 viii. All the data gathered in the system is saved and accumulated for future use, and might be shared with other security authorities in other sites. The data is saved both in local and in central data base.

ix. In case of need, the system has the ability to determine whether the subject has received the instructions, by making him actively respond to it. (For example, asking him to push a button in response to a question)

15 x. In order to increase reliability of the general test, the results are analyzed in a Fuzzy Logic process. This supports the testing procedure, which requires minimal interruption to the traffic, achieved by limited amount of tests given to each subject. Thus, the results are not absolute, but give a general direction whether the subject belongs – or not – to the suspects group. The grades are  
20 scaled from a total 0 that indicates that the subject was cleared – to 1, which identifies the subject as a suspect. The total of the ascription grades is summed up, and the result is defined as the grade compared to the criterion that indicates a potential suspect.

25 xi. The data saved in the system Data Base includes all kinds of information that might be relevant to the decision, such as: General data from current and prior measurements, historical and site data, medical data, intelligence information, and any other information that uses as a criterion.

The specified remarks are not binding and other and/or variants are applicable, depending upon the particular application.

5 B. Reliability tests for employees of sensitive organizations  
(Banks, governmental institutes, etc.)

B.1 General

10 The employee is tested at the beginning of his work, by filling a biographic and associative computerized questionnaire (for example: Word Association Test, from the guide written by D. Rapaport, M. Gill, and R. Schafer) that might include biometric and physiological measuring tools. This information is gathered and analyzed, and uses the system as data base during  
15 the reception process and later, for on-going supervision. It also provides a way to locate candidates with hidden intents, before accepting them into the organization.

After a while, periodically or randomly, the employee is asked to answer a computerized questionnaire. This can be done at his seat, or at a special  
20 location, in a fixed or changing manner and in relation to his position, his history, and any other information known to the system. For example a bank employee that his current position is loans confirmation, and used to work as a teller, is checked by the system in consideration with his professional past, his personal data (such as financial background) and general information  
25 which is not directly related to him (such as a suspicion of a fraud in the bank that wasn't located yet).

The system stores the data for future use.

B. 2. Bank, locating a fraud (example)

30

- a. The tested employee is seated in front his personal computer.
- b. During the test the camera inside the computer screen, which usually uses for communication, operates as a measuring tool detecting pupil size, facial expressions and temperature. The communication microphone also changes

into a sensor, recording the employees' voice in order to detect stress through voice stress analysis.

- c. As the test begins, before the employee is aware of it, the system conducts first measurement of the pupil, face and voice. The data is stored and defined as an Active Base Line. This parameter refers also to the Base Line which already exists in the system data base.
- d. By now, the system can analyze, even without the test, the person's psycho-physiological status.
- e. Following the measurement, over the screen appears: "This is a routine procedure. Please answer the following questionnaire by pressing the computer mouse". (As a calming, open manipulation)
- f. Later on, a set of questions is presented over the screen, including some that analyze the employees' association alignment (tested against his stored Base Line), and also camouflaged questions that are in fact a set of manipulations, which can be: open/concealed, stressing/calming, active/passive, etc.
- g. The employee answers the questions as requested. Before, within, or after the answering process, the system conducts an additional set of measurements that are chosen by the computer of the system. In some cases, the system might find a test irrelevant to a subject, such as pupil size analysis when the subject is wearing heavy gasses, fingerprints testing for a subject who suffered burn injuries, etc.
- h. All the data is stored in the system and defined as Test Data. The system analyzes the information, and compares it against the existing data (Base Line and Active Base Line). In case of suspicion, the system might instruct the employee to stay seated and wait for a supervisor. That alone is an extremely stressing manipulation, and the reaction to it can also be checked by the system.

Those versed in the art will readily appreciate that the invention is not bound by this specific sequence of operations of this non limiting example.

## DRAWING EXPLANATIONS

Drawing #1 illustrates a flow chart of generalized sequence of test selection operation, in accordance with an embodiment of the invention;

5 With the beginning of the process (101), the system loads a list of subsystems available at the site (102). The list changes according to the specific requirements of each site. Next stage is defining the target/s (103). For example, if the target is drugs dealers, the system adds to the physiological – behaviorist measuring tools also drugs sniffers, etc. That effects also the random choosing of the elements  
10 participating in the test (as pupil size meter, heroin sensor, etc.)(104). Following, the system turns into defining the actual procedure (Activating an early manipulation, activating a manipulation in test point #1 and not in # 2, etc.) (106) after the system has completed defining the parameters of the test procedure, it begins the actual test (107).

15

Drawing #2 illustrates a flow chart of generalized sequence of test selection operation, in accordance with an embodiment of the invention;

The procedure continues from stage #(107) in drawing #1.

20 The test starts, and at the first test point the system considers whether to activate a manipulation at that first step (202). If not, it immediately activates the first measurement (204). In case the system decided to start with the manipulation (203), it conducts the first measurement right after it (204). The test results are stored in the system for later use.

25 At the following stage, the system again considers whether to activate a manipulation at that stage (205). If not, the second measurement is performed immediately (207). If the system decided to present a manipulation (206), it activates the second measurement immediately after (207). The data of the second test is also stored in the system, and analyzed (208). The analysis results are forwarded (209).

30

Drawing #3 illustrates a generalized block diagram of exemplary system architecture, in accordance with an embodiment of the invention.

The subject (301), as entered to the test, might be exposed to a manipulation (302). As soon as he enters the site, the subject presents his documents, as well as



his fingerprints for identity verification, and physiological and behaviorist tests dictated by the computer through the screen (303, 306). The subject is photographed by a camera (305), and after passing the first step, continues into a path of screening systems (305). Following, he goes through the security gate (307). At the process, the subject passes a security inspector that stands inside a protected booth (308). All the measuring parameters and the tests results are transferred to the computer (309) and the monitor (310) for later process and analysis. The computer also controls the manipulation choosing system, etc.

The physical structure of the second test (311-317) is similar, and might be conducted at the same facility.

In accordance with various embodiments of the invention there are provided,

1. The system is designed to locate individuals with hidden intent.
2. The system has at least two different measurement steps that measure behaviorist and/or physiologic parameters.
3. The system activates a manipulation, which is intended to create a change in the measured parameters, before, or during, one of the measures.
4. The manipulation might be open or concealed.
5. The manipulation might be conscious or subconscious.
6. The manipulation might be active or passive.
7. The manipulation might be stressing or calming.
8. The manipulation might be random or scheduled.
9. The manipulation matches the wanted target (focused on the targeted population, in order to create physiological and behaviorist changes only within that population, and by so separate the wanted elements from the general public).
10. The system might include means to assure that the subject absorbed the manipulation (for example, the system instructs him to press a button in response to a question, which is actually a concealed manipulation).
11. Besides data from internal sources, the system might receive data from external sources as well (for example, external data bases as of the borders administration, or external systems as luggage screening systems).
12. As a result of the data process, the system decides whether to detain the subject for an extensive enquiry.

13. The system is an adaptive system, and uses the accumulative data base for on going improving of its abilities.

14. The system is modular, and can interface with a variety of completing systems.

5 The invention has been described with a certain degree of particularity, but those versed in the art will readily appreciate that various alterations and modifications may be carried out, without departing from the scope of the following Claims:

10

## **CLAIMS:**

1. A method for screening individuals with hidden intent, comprising:
  - a) providing at least two tests and at least one manipulation between at least  
5 two of said tests
  - b) obtaining test measurements of the individual in respective tests before and after the at least one manipulation;
  - c) providing indication on hidden intent of the individual in the case that test measurement parameters after manipulation meet a predetermined criterion.
- 10 2. The method of Claim 1, wherein at least one of said manipulations is selected randomly from a manipulation bank.
3. The method according to Claims 1 or 2, wherein at least one of said  
15 manipulations being open or concealed.
4. The method according to anyone of Claims 1 to 3, wherein at least one of said manipulations being stressing or relaxing.
- 20 5. The method according to anyone of Claims 1 to 4, wherein at least one of said manipulations creating conscience reaction or creating sub conscience reaction.
6. The method according to anyone of Claims 1 to 5, wherein at least one of said manipulations being targeted or being general.
- 25 7. The method according to anyone of the preceding claims, for use in an airport for locating drugs smugglers.
8. The method according to anyone of claims 1 to 6, for use in reliability tests for  
30 employees of sensitive organizations.
9. A method for screening individuals with hidden intent, comprising:
  - a) Providing at least two tests and at least one manipulation between at least  
two of said tests

b) Obtaining test measurements of the individual in respective tests before and after the at least one manipulation;

c) Providing indication on hidden intent of the individual in the case that test measurement parameters after manipulation meet a predetermined criterion,

5 irrespective of whether the individual attempts to conceal the hidden intent.

10. The method according to anyone of claims 1 to 6, for use in public places for locating terrorists.

10 11. The method according to anyone of claims 1 to 6, for use in public places for locating criminals.

12. The method according to anyone of claims 1 to 6, for use in security tests for crowds in public places.

15

For the Applicants,  
**REINHOLD COHN AND PARTNERS**  
By:

20

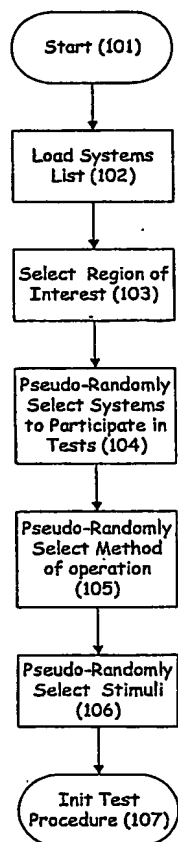


Figure 1 - Test(S) Selection Mechanism

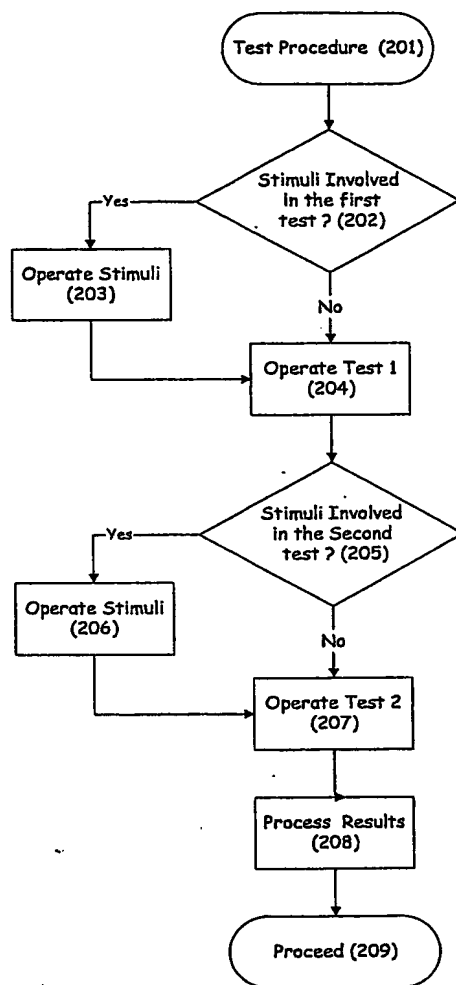


Figure 2 - 2 Steps Test Example

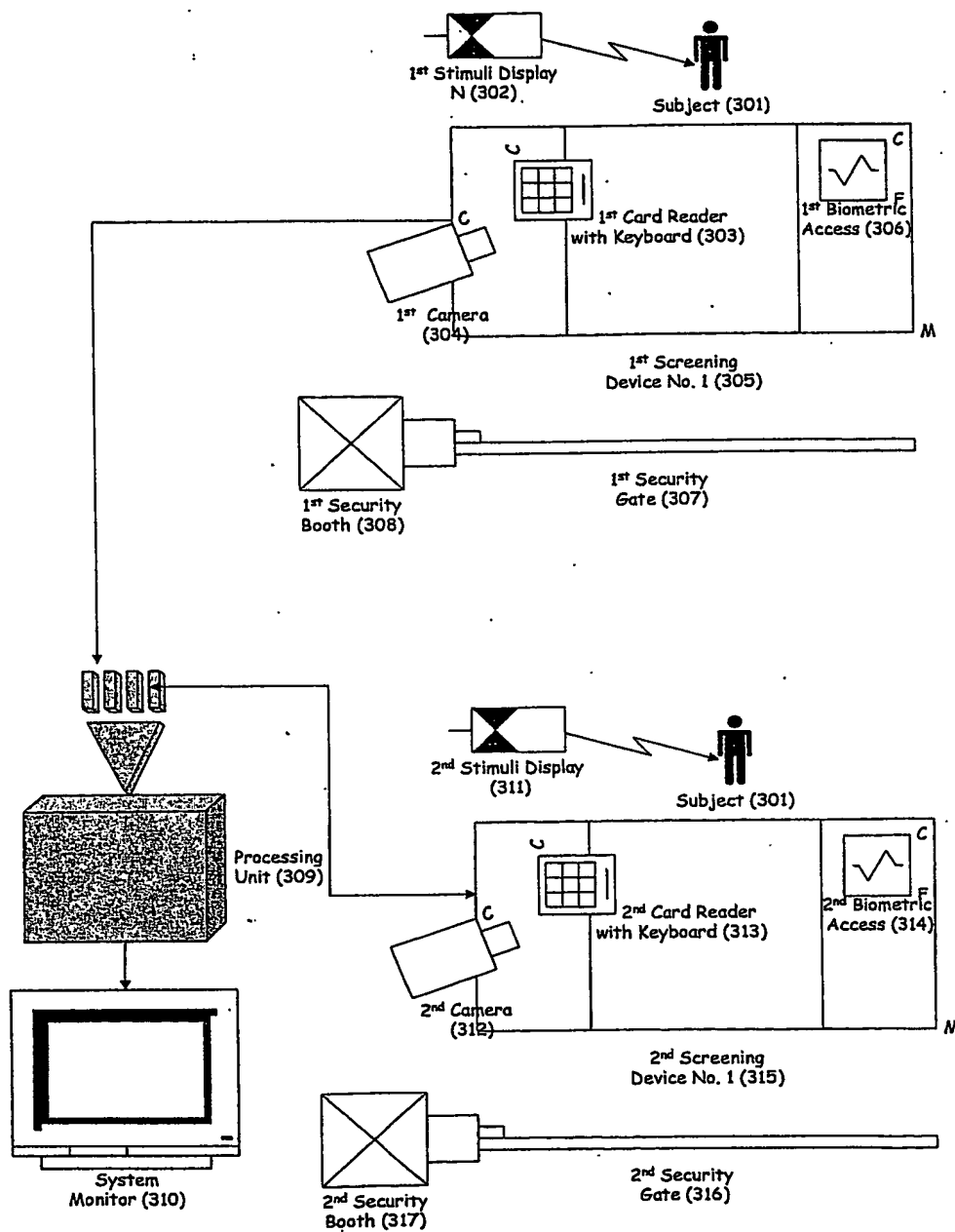


Figure 3 - 2 Steps Test System Block Diagram  
Example